Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	219.38420X00
First Inventor or Application Identifier	James L. Jason, Jr. et al.
Title	COMMUNICATION SYSTEM INCLUDING A SECURITY SYSTEM
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] * Fee Transmittal Form (e.g., PTO/SB/17) (Submit an original and a duplicate for fee processing)
2. [X] Specification [Total Pages 12] (preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings (if filed)
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. [X] Drawing(s) (35 U.S.C. 113) [Total Sheets 4]
4. Oath or Declaration [Total Pages]
   a. [ ] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 C.F.R § 1.63(d)) (for continuation/divisional with Box 16 completed)
      i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

5. [ ] Microfiche Computer Program (Appendix)
6. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
   a. [ ] Computer Readable Copy
   b. [ ] Paper Copy (identical to computer copy)
   c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. [ ] Assignment Papers (cover sheet & document(s))
8. [ ] 37 C.F.R.§3.73(b) Statement (when there is an assignee) [ ] Power of Attorney
9. [ ] English Translation Document (if applicable)
10. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
11. [ ] Preliminary Amendment
12. [X] Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
13. [ ] * Small Entity Statement(s) [ ] Statement filed in prior application Status still proper and desired (PTO/SB/09-12)
14. [ ] Certified Copy of Priority Document(s) (if foreign priority is claimed)
15. [ ] Other: .....

* NOTE FOR ITEMS 1 & 13 IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment.

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: _____/_____

Prior application information: Examiner _____ Group / Art Unit: _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[X] Customer Number or Bar Code Label 020457 (Insert Customer No. or Attach bar code label here) or [ ] Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Fax	

Name (Print/Type)	James N. Dresser	Registration No. (Attorney/Agent)	22,973
Signature		Date	June 29, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

jc835 U.S. PTO 09/605361 06/29/00

jc835 U.S. PTO 06/29/00

219.38420X00
P8770

UNITED STATES PATENT APPLICATION FOR:

COMMUNICATION SYSTEM INCLUDING A SECURITY SYSTEM

Inventors:

James L. JASON, Jr.

Ylian SAINT-HILAIRE

Prepared by:

Antonelli, Terry, Stout & Kraus, LLP
1300 North 17th Street, Suite 1800
Arlington, VA 22209
Tel: (703) 312-6600
Fax: (703) 312-6666

COMMUNICATION SYSTEM INCLUDING A SECURITY SYSTEM

FIELD

The present invention pertains to a security system for connecting a client application to a communication network. More particularly, the present invention relates to controlling the security association on an application on a socket of a communication network.

BACKGROUND

Communication on computer networks is frequently done utilizing secure communication techniques. By way of example, people frequently purchase goods and services over the Internet utilizing secure communications links. Data transferred over such a secure link is described by an Internet Protocol (IP) address, protocol, and ports, and a security association is established using an Internet Protocol Security (IPsec) protocol. The security association continues until it is no longer needed. Generally, an IPsec security association lasts until either a specified amount of traffic has been transmitted using the association or a specified amount of time has passed. These techniques of determining the duration of the security association are sufficient for long-lived security associations that may be renegotiated multiple times. However, a person contacting a web site over the Internet utilizing, for example, a home computer to make a purchase, generally does not visit that web site for an extended period of time before moving on, either by going to another web site or by closing the connection to the Internet. After such a client has left the web site, the IPsec driver for the web site maintains the security association as active. Lifetime management

based on the amount of traffic or the amount of time thus results in the security association being maintained for longer than is necessary. One solution to this is for the IPsec driver to periodically remove idle security associations which have not been used to protect any inbound traffic for some predetermined amount of time. However, this may expire security associations that are still in use, for example, by someone merely observing activity on a web site. In any event, this idle detection could be made more efficient and could be done in a more timely manner if the IPsec driver had some context information it could correlate with the security association.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention are more apparent from the following detailed description and claims, particularly when considered in conjunction with the accompanying drawing. In the drawings:

FIG. 1 is a block diagram of a communications system that might utilize a security system in accordance with the present invention;

FIG. 2 is a block diagram of a security system for connecting a client to a communication network in accordance with an embodiment of the present invention;

FIG. 3 is a flowchart of a method of controlling applications on a computer network in accordance with an embodiment of the present invention; and

FIG. 4 is a more detailed block diagram of an embodiment of one step in the flow chart of FIG. 3.

DETAILED DESCRIPTION

FIG. 1 depicts a communications system, including a workstation or personal computer 10, which communicates with a server 12 by means of a communication network 14 such as the Internet. In accordance with the present invention, the connection between workstation/personal computer 10 and server 12 might be a secure link on the communication network 14.

FIG. 2 depicts the security system in accordance with an embodiment of the present invention. Within workstation/personal computer 10, a network interceptor 20 is positioned between an application 22 and a Transmission Control Protocol/Internet Protocol (TCP/IP) stack 24 so as to gather context information. TCP/IP stack 24 is coupled to a communication network, such as network 14, by Internet Protocol security (IPsec) packet classifier 26. IPsec packet classifier 26 is responsible for performing the IPsec processing on incoming and outgoing packets. When application 22 wishes to send or receive data to or from an application on server 12, or to another computer reachable via network 14, application 22 uses a socket on network 14. The position of network interceptor 20 permits the network interceptor to be aware of all socket operations performed by application 22. In particular, network interceptor 20 monitors when application 22 closes the socket.

When IPsec packet classifier 26 detects that a secure communication is desired, it negotiates with a security association negotiator 28 to provide the necessary secure link. Security association negotiator 28 might be the Internet Key Exchange (IKE) negotiator, for example. When a security association is established, security association negotiator 28 notifies network interceptor 20, which assures that the appropriate security association information is available to IPsec packet classifier 26. In addition, network interceptor 20 maintains a

reference to the security association on the socket. The security association, of course, is not unique to its particular socket but may apply to all applications between workstation/personal computer 10 and server 12. When additional sockets are created that will be protected by an existing security association, network interceptor 20 monitors this.

FIG. 3 is a flowchart of an embodiment of a method of controlling security on a communication network connecting a server and a client in accordance with the present invention. In a step S1, application 22 creates a connected socket. As a consequence, in step S2, network interceptor 20 correlates the socket with an appropriate security association. FIG. 4 is a detailed flowchart of this step. In FIG. 4, in step S2a, it is determined whether there is an active security association that would cover the traffic of the socket. If not, then in step S2b, a security association is established. In step S2c, the security association information is given to the IPsec packet classifier; and in step S2d, the driver gives back a handle. In step S2e, the security association and handle are correlated with the socket, and the usage count is incremented. In step S2a, if there already exists an active security association that would cover the traffic from the socket, then the flow proceeds directly to step S2e to correlate that security association and handle with the socket and increment the usage count.

Returning to FIG. 3, once the socket is correlated with the appropriate security association in step S2, then the application uses the socket in step S3. When the communication is completed, the application closes the socket in step S4. In step S5, it is determined whether any other sockets are using the security association. If so, then the process ends for the socket of the completed application. However, in step S5, if it is determined that no other sockets are using the security association, then in step S7, the driver is instructed to delete the security association, following which the process ends in step S6.

Accordingly, once no sockets are using the security association, the security association is deleted.

When the last socket for a particular security association is closed, network interceptor **20** can immediately delete the security association so that the IPsec packet classifier will no longer perform IPsec processing on packets which match the security association packet flow parameters. Alternatively, network interceptor 20 can mark the security association as currently no longer needed. Network interceptor 20 will then periodically make a sweep of security associations and delete those that have not been used for some predetermined, configurable time. Thus, for example, when server **12** has fulfilled the client request from workstation/personal computer **10**, server **12** closes the socket used to communicate with the workstation/personal computer. When workstation/personal computer **10** makes another request, a new socket is created. If the security association is retained for a small period of time, during which such a new socket is created, that security association can be used, forgoing the security association negotiation of steps S2b, S2c, and S2d in FIG. 4.

By utilizing the present invention, the IPsec driver no longer is required to dedicate a thread to performing the housekeeping function of deleting idle security associations. Security associations may be deleted as soon as they are no longer needed. As a consequence, valuable non-paged memory space is saved in the driver, as it no longer has to retain information of unneeded security associations. Context information associated with the network flow can be used as the determining factor when deleting security associations. Alternatively, other context information could be used. For example, a system may have a set of IP policies it enforces when no user is logged in. A network interceptor at the applications level can monitor log-in

of new users and immediately delete security associations as such a new users policy may be different and would require a security association with different security parameters.

The present invention can be implemented in hardware, firmware, or software, and for example, might be maintained in a storage medium such as a magnetic or an optical storage medium, or any other medium capable of storing the invention.

Although the present invention has been described with reference to preferred embodiments, numerous rearrangements, alterations, and substitutions could be made, and still the result would be within the scope of the invention.

WE CLAIM:

1. A method of controlling a security association of a network communication between a local application and a remote application, the local application utilizing a socket, said method comprising:

(a) monitoring a completion status of the communication;

(b) upon completion of the communication, closing the socket; and

(c) in response to closing of the socket, terminating a correlation of the security association with the socket.

2. A method as claimed in claim 1, wherein step (c) comprises deleting the security association.

3. A method as claimed in claim 1, wherein step (c) comprises determining whether any other socket is correlated with the security association, and when it is determined that no other socket is correlated with the security association, deleting the security association.

4. The method of claim 1, wherein the application operates through a driver, and step (c) includes notifying the driver that the security association is no longer needed, to cause the driver to terminate the correlation.

5. A method of controlling communication between a local application and a remote application on a communication network, said method comprising:

(a) creating a socket for the local application;

(b) correlating the socket with a security association;

(c) performing the communication through the socket and the communication network;

(d) upon completion of the communication closing the socket; and

(e) in response to closing of the socket, terminating the correlation of the security association with the socket.

6. The method of claim 5, wherein step (b) comprises:

(1) determining whether there is an active security association that would cover traffic for the socket;

(2) if step (1) determines that there is an active security association that would cover traffic for the socket, then correlating the socket with the active security association;

(3) if step (1) determines that there is not an active security association that would cover traffic for the socket, then:

(i) determining a security association for traffic for the socket;

(ii) giving the determined security association to a network security driver;

(iii) receiving a handle for the security association from the network security driver; and

(iv) correlating the socket with the security association of the handle.

7. A method as claimed in claim 5, wherein step (e) comprises deleting the security association.

8. A method as claimed in claim 5, wherein step (e) comprises determining whether any other socket is correlated with the security association, and when it is determined that no other socket is correlated with the security association, deleting the security association.

9. The method of claim 5, wherein the application operates through a driver, and step (e) includes notifying the driver that the security association is no longer needed, to cause the driver to terminate the correlation.

10. A security system for connecting a client application to a communication network, wherein said security system comprises:

a transmission control protocol for controlling communication between the client application and the communication network;

a security classifier for coupling said transmission control protocol to the network, said security classifier determining a security classification for the client application;

a security association negotiator responsive to the client application opening a socket at a node of the communication network, for correlating the socket with a security association based on the determined security classification; and

a network interceptor coupling the client application with the transmission control protocol, and responsive to the socket being closed for terminating the correlation of the socket with the security association.

11. A security system as claimed in claim 10, wherein the network interceptor responds to the socket being closed by deleting the security association.

12. A security system as claimed in claim 10, wherein the network interceptor responds to the socket being closed by determining whether any other socket is correlated with the security

association, and when it is determined that no other socket is correlated with the security association, deleting the security association

13. A communication system, comprising:

a communication network, including a plurality of nodes;

a server connected to a first one of said nodes;

a client processor;

a storage medium within said client processor and storing a security system for connecting said client processor to said communication network for communication with said server, wherein said security system includes a transmission control protocol for controlling communication between said client processor and said communication network; a security classifier for coupling said transmission control protocol to said communication network, said security classifier determining a security classification for said client processor; a security association negotiator responsive to said client processor opening a socket at a node of said communication network, for correlating the socket with a security association based on the determined security classification; and a network interceptor coupling said client processor with said transmission control protocol, and responsive to the socket being closed for deleting the security association

14. A communication system as claimed in claim 13, wherein the network interceptor responds to the socket being closed by deleting the security association.

15. A communication system as claimed in claim 13, wherein the network interceptor responds to the socket being closed by determining whether any other socket is correlated with

the security association, and when it is determined that no other socket is correlated with the security association, deleting the security association.

16. An article, comprising a storage medium having instructions stored thereon, the instructions when executed controlling a security association of a network communication between a local application and a remote application, the local application having a socket, by monitoring a completion status of the communication; upon completion of the communication, closing the socket; and in response to closing of the socket, terminating a correlation of the security association with the socket.

17. An article as claimed in claim 16, wherein the correlation of the security association with the socket is terminated by deleting the security association.

18. An article as claimed in claim 16, wherein the correlation of the security association with the socket is terminated by determining whether any other socket is correlated with the security association, and when it is determined that no other socket is correlated with the security association, deleting the security association.

19. An article as claimed in claim 16, wherein the application operates through a driver, and the correlation of the security association with the socket is terminated by notifying the driver that the security association is no longer needed, to cause the driver to terminate the correlation.

ABSTRACT OF THE DISCLOSURE

A communication system including a security system, and a method of controlling a communication system. The communication system includes a communication network having a plurality of nodes, a server connected to a first one of the nodes, and a client processor. A magnetic medium within the client processor stores the security system for connecting the client processor to the communication network for communication with the server. The security system includes a transmission control protocol for controlling communication between an application on the client processor and the communication network and a security classifier for coupling the transmission control protocol to the communication network and determining a security classification for the client processor. A security association negotiator is responsive to the client processor opening a socket at a node of the communication network, for correlating the socket with a security association based on the determined security classification. A network interceptor couples the client processor with the transmission control protocol and is responsive to the socket being closed for deleting the security association. In accordance with the method, the completion status of the communication is monitored. Upon completion of the communication, the socket is closed, and in response to closing of the socket, the correlation of the security association with the socket is terminated.

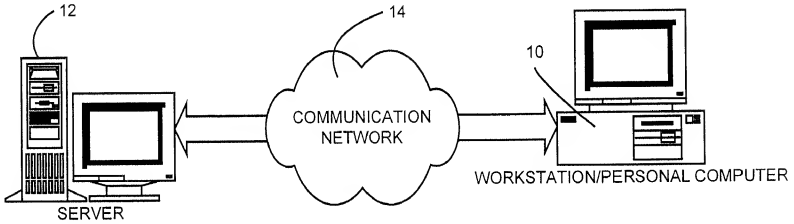
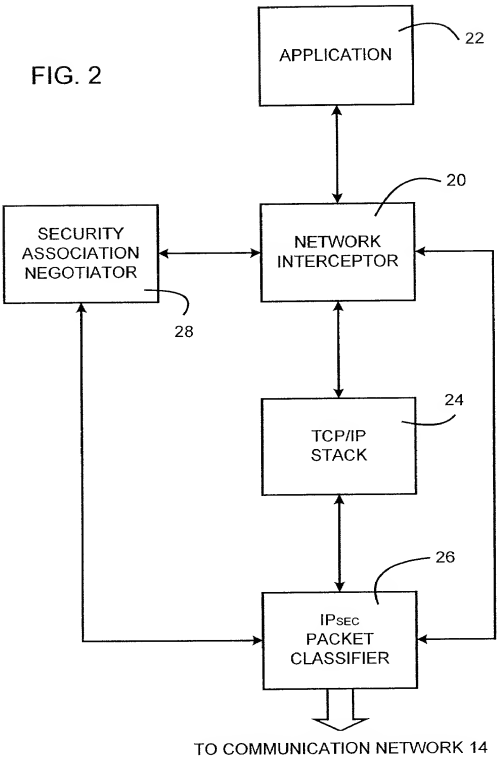


FIG. 1

FIG. 2


APPLICATION
22
20
SECURITY ASSOCIATION NEGOTIATOR
NETWORK INTERCEPTOR
28
24
TCP/IP STACK
26
IPSEC PACKET CLASSIFIER
TO COMMUNICATION NETWORK 14

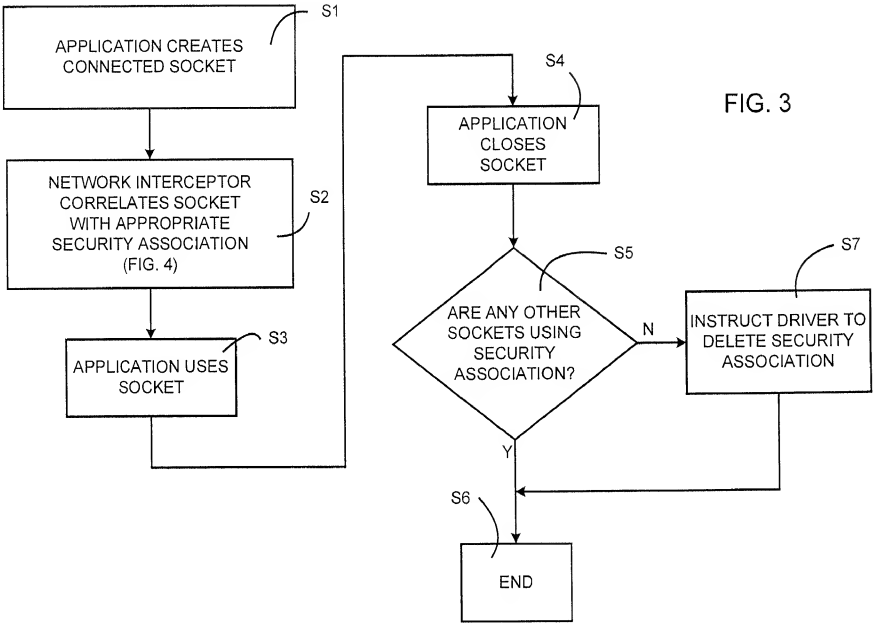

APPLICATION CREATES CONNECTED SOCKET
S1
NETWORK INTERCEPTOR CORRELATES SOCKET WITH APPROPRIATE SECURITY ASSOCIATION (FIG. 4)
S2
APPLICATION USES SOCKET
S3
APPLICATION CLOSES SOCKET
S4
ARE ANY OTHER SOCKETS USING SECURITY ASSOCIATION?
S5
N
Y
INSTRUCT DRIVER TO DELETE SECURITY ASSOCIATION
S7
END
S6

FIG. 3

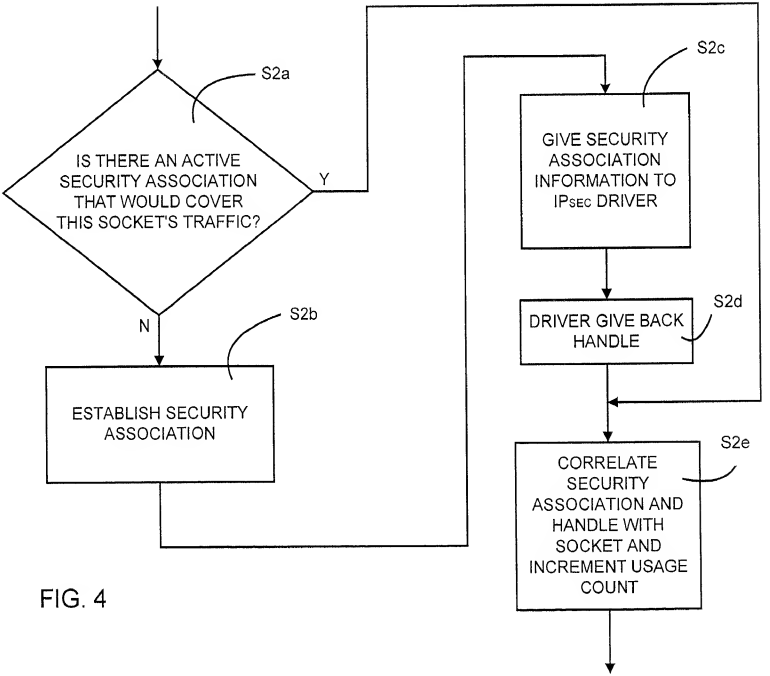


FIG. 4